Affects Members Of the Public? ☐

Department of Energy

Privacy Impact Assessment (PIA)

Guidance is provided in the template. See DOE Order 206.1, Department of Energy Privacy Program, Appendix A, Privacy Impact Assessments, for requirements and additional guidance for conducting a PIA: https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder/@@images/file

Please complete form and return via email to Privacy@hq.doe.gov

No hand-written submissions will be accepted.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	5/1/2024
Departmental Element & Site	Bonneville Power Administration (BPA) HQ, 905 NE 11th Ave, Portland, OR
Name of Information System or IT Project	Transmission Identity Manager (TIM)
Exhibit Project UID	BPA is a Non-Appropriated Federal agency and is exempt from Exhibit 300 submissions
New PIA ☒ **Update** ☐	This is a new PIA for a new system.

	Name, Title	Contact Information Phone, Email
Information System Owner	Lance Dawkins, TTOV Transmission Technology Infrastructure Manager	360-418-4361 ladawkins@bpa.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Information Owner	Kim Hunter, TT Transmission Technology Director	360-619-6715 kahunter@bpa.gov
Local Privacy Act Officer	Candice Palen Privacy Act Officer	503-230-5602 cdpalen@bpa.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Rustin Jones Information System Security Engineer	360-418-2228 rpjones@bpa.gov
Person Completing this Document	Rustin Jones Information System Security Engineer	360-418-2228 rpjones@bpa.gov
Purpose of Information System or IT Project	The Transmission Identity Manager (TIM) project will create a Transmission (T) Organization program that manages cyber and physical access, revocation and tracking/archiving of information (for the purposes of Identity Credential Access Management (ICAM)). TIM will support compliance with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) program 004 standards to operate with effective checks and balances pertaining to management of access/revocation activities to physical and cyber assets. The CIP program is mandatory for any organization or "responsible entity" that comes under the electricity segment of the energy sector. TIM ensures a long-term structure to document cybersecurity and physical asset access. Compliance with NERC CIP standard 004, which documents personnel and training. The specifics of the standards require that personnel accessing systems are vetted, that the vetting and access are documented, that the access is regularly reviewed and those who no longer require access are removed within 24 hours for those terminated for cause and within 7 calendar days of any change of personnel with access to Critical Cyber Assets. TIM includes data retrieval and analysis through both scheduled and unscheduled reports as well as the ability to perform internal audits related to access. TIM retrieves lists of personnel with access to facilities and logical systems. These reports include system logs as well as access logs. The information included on the reports includes name, work email, work facility accessed in the course of work (this may include work address and work phone number). The system also includes BPA User Domain Identification number commonly referred to as BUD ID, the Human Resource Management Information System Identification number commonly referred to as HRMIS ID, or other system designated number. The system stores information about devices and users, verifies identities and privileges, and defines access rights to networked resources. The system is on premises and only accessed by BPA personnel.	

MODULE I – PRIVACY NEEDS ASSESSMENT

Type of Information Collected or Maintained by the System:	☐ SSN Social Security number ☐ Medical & Health Information e.g. blood test results ☐ Financial Information e.g. credit card number ☐ Clearance Information e.g. "Q" ☐ Biometric Information e.g. finger print, retinal scan ☐ Mother's Maiden Name ☐ DoB, Place of Birth ☐ Employment Information ☐ Criminal History ☒ Name, Phone, Address – work only ☒ Other –login ID (Bonneville User Domain (BUD) ID), system specified user ID, HRMIS ID
Has there been any attempt to verify PII does not exist on the system? **DOE Order 206.1, *Department of Energy Privacy Program,* defines PII as** *any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.*	N/A, the above identified non-sensitive PII exists on the system.
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	N/A

Threshold Questions

1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	YES
2. Is the information in identifiable form?	YES

MODULE I – PRIVACY NEEDS ASSESSMENT

3. Is the information about individual Members of the Public?	NO
4. Is the information about DOE or contractor employees?	YES ☒ Federal Employees ☒ Contractor Employees

If the answer to **all** four (4) Threshold Questions is "**No**," you may **proceed to the signature page** of the PIA. Submit the completed PNA with signature page to the CPO.

Module II must be completed for all systems if the answer to any of the four (4) threshold questions is "Yes." All questions must be completed. If appropriate, an answer of N/A may be entered.

The goal of the threshold questions is to legitimately and efficiently determine whether additional assessment is necessary. If there is doubt, it is in the System Owner's best interest to complete Module II.

PIAs affecting Members of the Public are posted on the DOE Privacy website. For this reason, PIAs affecting Members of the Public should be written in plain language and at a high level so they are easily understandable and do not disclose sensitive information.

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

1. AUTHORITY **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	Department of Energy Authorization Act, Title 42 United States Code (U.S.C.) Section 7101, et seq. The Bonneville Power Project: Administrative Authority to Contract (16 U.S.C. §§ 832a(f), 839f(a)) grants the Bonneville Power Administration authority to procure contracts to advance the agency's mission.

MODULE II – PII SYSTEMS & PROJECTS

2. CONSENT

What opportunities do individuals have to decline to provide information (e.g. where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?

Only BPA employees and contractors will have access to the system. Consent is assumed from the initial login disclosure that all BPA system users agree to for access to the network.

3. CONTRACTS

Are contractors involved with the design, development and maintenance of the system? If yes, was the Privacy Order CRD or Privacy Act clauses included in their contracts?

Yes, the contract contains the necessary privacy act clauses.

4. IMPACT ANALYSIS:

How does this project or information system impact privacy?

The overall privacy risk is LOW – minimal non-sensitive PII is collected.

Confidentiality Factors	Low	Moderate	High
Identifiability	X		
Quantity of PII	X		
Data Field Sensitivity	X		
Context of Use	X		
Obligation to Protect Confidentiality	X		
Access to and Location of PII	X		
Overall Privacy Risk	X		

MODULE II – PII SYSTEMS & PROJECTS	
5. SORNs **How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?** **If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**	Yes, information can be retrieved by identifier (e.g. name, BUD ID, or system specified user ID.
6. SORNs **Has a Privacy Act System of Records Notice (SORN) been published in the *Federal Register*?** **If "Yes," provide name of SORN and location in the *Federal Register*.**	TIM is not used to collect sensitive information, but does access the individual's name, BUD ID number, and HRMIS ID number from the Human Resources Management Information System. The relevant SORN for data shared between HRMIS and TIM through Active Directory is **OPM/GOVT-1 General Personnel Records** (specifically role and organization data).
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	N/A
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	PII information comes from Active Directory, manual entry, and the Data Integration Layer.
9. Will the information system derive new or meta data about an individual from the information collected?	No
10. Are the data elements described in detail and documented?	Yes, the data elements are described in the Implementation Design document and will be included in the system security plan.
DATA USE	

MODULE II – PII SYSTEMS & PROJECTS	
11. How will the PII be used?	The system uses name, account ID, and employee type to track, grant, and revoke privileges in a timely manner.
12. If the system derives meta data, how will the new or meta data be used? **Will the new or meta data be part of an individual's record?**	N/A
13. With what other agencies or entities will an individual's information be shared?	DOE IG, Western Electric Coordinating Council (WECC), and North American Electric Reliability Corporation (NERC) during audits.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	The system tracks physical and cyber privilege access and the reports will allow BPA to track and monitor compliance. • WECC and NERC Compliance Reporting • Semi- Annual Review • Quarterly Access Verification
15. What will be the use of these reports?	As evidence of compliance with WECC and NERC requirements and to ensure that access is being granted, transferred, and revoked properly and in a timely manner.
16. Who will have access to these reports?	BPA Managers, system administrators, database administrators, TIM program personnel.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	Yes, TIM will monitor an individual's accounts and assigned privileges to control center systems.
18. What kinds of information are collected as a function of the monitoring of individuals?	User IDs, HRMIS IDs, and system access information.

MODULE II – PII SYSTEMS & PROJECTS	
19. Are controls implemented to prevent unauthorized monitoring of individuals?	System configuration. Only authorized users with assigned privileges can access the system data.
DATA MANAGEMENT & MAINTENANCE	
20. How will records about individuals be kept current and verified for accuracy, relevance and completeness? Include PII data collected from sources other than DOE records.	Data is kept current and accurate via Active Directory, manual verification, data feed syncs, Quarterly Access Verifications, and Semi Annual Reviews.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	N/A
Records Management	
22. Identify the record(s).	Cyber and Physical access privileges, user identities, and non critical PII.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	Check appropriately and cite as required. ☐ Unscheduled ☒ Scheduled *(cite NARA authority(ies) below)* GRS 4.2.030, SR-1130 destroy 2 years after submission of report, but longer retention is authorized if required for business use.
24. Records Contact	IGLM@bpa.gov
ACCESS, SAFEGUARDS & SECURITY	
25. What controls are in place to protect the data from unauthorized access, modification or use?	The System Owner has implemented the required security controls in accordance with its FIPS 199 categorization.

MODULE II – PII SYSTEMS & PROJECTS	
26. Who will have access to PII data?	Roles will be documented in the Account Management Plan BPA Managers, system administrators, Resource Managers, database administrators (DBAs), and program personnel (individuals with access for the purpose of processing access/revocation requests, privilege reviews, and running reports for audit purposes).
27. How is access to PII data determined?	User Access is restriced by assigned roles.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	No
29. For connecting information systems, is there an Interconnection Security Agreement (ISA) or other agreement between System Owners to ensure the privacy of individuals is protected?	No, the system does not connect to external systems.
30. Who is responsible for ensuring the authorized use of personal information?	Information Owner
END OF MODULE II	

SIGNATURE PAGE

	Signature	Date
System Owner	(Print Name) LANCE DAWKINS Digitally signed by LANCE DAWKINS Date: 2024.09.04 08:35:20 -07'00' (Signature)	
Information Owner	(Print Name) KIMBERLY HUNTER Digitally signed by KIMBERLY HUNTER Date: 2024.09.04 11:48:39 -07'00' (Signature)	
Local Privacy Act Officer	(Print Name) CANDICE PALEN Digitally signed by CANDICE PALEN Date: 2024.09.04 12:13:40 -07'00' (Signature)	
DOE Chief Privacy Officer	(Print Name) WILLIAM HUNT Digitally signed by WILLIAM HUNT Date: 2024.08.13 10:07:12 -04'00' (Signature)	